REMARKS/ARGUMENTS

The present application provides a method for creating, storing and reading a new certificate types for certification of several keys. These new certificate types are particularly applicable to shere there is limited storage capacity, such as in the case of chipcards. The new certificate types include basic, group and supplementary certificate types that are issued in various combinations. In the case of basic and supplementary certificate combinations, redundant fields for several keys are placed in one basic certificate and separate supplementary certificates are issued for each key, each supplementary certificate containing a reference to the basic certificate and data fields that differ from key to key. The basic and supplementary forms of certification can be used where certificates are issued at different times for the same user by the same certification body providing great flexibility with the use of these new certificate types. Where several keys are to be issued at the same time, for the same duration, to the same user, by the same certification authority, a group certificate can be issued. By means of the group certificate, all data elements for a set of several keys subject to certification are grouped into one certificate. The use of all these new certificate types substantially reduces the memory requirement, and handling of the certificates is simplified for the communication partners.

Claim Rejections Under 35 USC 103

A. Claims 1 to 12 were rejected under 35 USC 103(a) as being unpatentable over VeriSign "Certificate Practice Statement", version 1.2, in view of Sutter, U.S.

patent #5,924,094, Stallings "Cryptography and Network Security", 2nd Edition, Karlton "Proposal to Add Attribute Certificates to TLS 3.1" and Silberschatz et al., "Database System concepts 3rd Edition.

Applicant's attorney found nothing in any of the references of the recited combination that teaches combining redundant information for several keys into one group certificate or issuing a basic certificate and then issuing supplementary certificates at different times for each of several keys. With respect to supplementary certificates, the Examiner points out that VeriSign does not teach the use of a supplementary certificates for the issuance of additional keys and relies on the teachings of the Sutter patent and the Karlton reference to provide the missing teaching. However, the subject matter cited in column 49, lines 35 to 39, in the Sutter patent does not mention issuance of supplementary certificates and Karlton clearly states that what is described in the article as an "attribute cert" shall have no associated key pair and cannot be used to establish identity. Therefore, the Karlton teaching specifically excludes use of its attribute cert for applicant's purposes. Moreover, the author of the article is unsure how his idea is to be implemented. The article was published in 6/26/96 and it is unclear from the record if it was implemented or even implementable for its limited purpose. However, we do know that the attribute certificate "can't be used to establish identity." Accordingly, there not only is a lack of teaching applicant's invention in the proposed combination of Verisign, Sutter and Karlton, but a specific exclusion of any such teaching of the combination for the purposes proposed by applicant in view of Karlton's express statements about configuration and limitation and use of attribute certs. Without the issuance of further keys in

applicant's supplementary certificates, the advantages in accordance with this aspect of the applicant's invention cannot be obtained.

With respect to group certificates, the Examiner's contention in paragraph 11a of his action that VeriSign discloses a certificate designed to carry a number of data elements for a plurality of keys, applicant's attorney found no such mention of use of VeriSign certificates for redundant elements in connection with multiple keys. Further, Sutter patent citation in column 49 does not say how a certificate is to be configured to cover multiple keys. Therefore there is no teaching in the cited combination for the configuration of a group certificate designed to support or carry multiple keys, as described in the present application.

In addition to the failure of the references to disclose a proper combination of patents to meet the applicant's disclosed invention, the Examiner fails to provide evidence of any suggestions in the references or otherwise (as the time of applicant's invention) to combine and modify the references as suggested by the Examiner. The reasons that the Examiner gives for it being obvious to make the combinations the Examiner proposes essentially breaks down to the need for applicant's invention. That is, it appears that what the Examiner is saying is that in view of this great need, those skilled in the art would go through the numerous references in the field, pick out the same five references the Examiner has chosen, then modify them just as the Examiner has done and then combine them so as to meet every detail in every one of the claims of the application. This is an unlikely scenario. It appears that what the Examiner has done in his rejection is use hindsight of applicant's disclosure to select certain, otherwise unconnected,

references out of a multiplicity of such references and then piece them together and modify them using the applicant's disclosure as an instruction manual and the claims in the application as templates to piece together the teachings of these modified references. The arguments presented by the Examiner for nonpatentability are more applicable to the unobviousness of the applicant's invention since even with all the advantages attributed by the Examiner to the applicant's invention, a teaching of that invention is not found in a single reference.

B. Claims 13 to 18 were rejected under 35 USC 103(a) in view of the combination cited in A further in view of the Deo, U.S. patent #5,721,781.

The addition of the Deo patent to the combination cited in A does not change the failure of the combination cited by the Examiner in A to teach applicant's invention. Further, the cited sections of Deo do not specifically teach storing and retrieving basic and supplementary certificates in a nonvolatile memory of a chip card. Claim 17, cited in this section, is not limited to a chip card.

C. Claims 19 to 25 were rejected over the prior art cited against claims 1 to 7 in A further in view of "JAVA XZ509 Certificates and Certificate Revocation Lists." The arguments presented in A with respect to claims 1 to 7 apply equally well to the Examiner's position with respect to rejection of claims 19 to 25 in B and C.